

**INTHE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI**

**IN THE MATTER OF THE
SEARCH OF:
2390 HIGHLANDVILLE ROAD
OZARK, MISSOURI**

18-SW-2022DPR

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeffrey Burnett, a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

1. I have been employed as a police officer with the City of Springfield, Missouri, since May 1999. I am currently a TFO with the FBI, as well as a member of the Southwest Missouri Cyber Crimes Task Force. I have been assigned to investigate computer crimes to include violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and every day work related to conducting these types of investigations. I have attended training provided by the FBI Cyber Crime Division, the FBI's Regional Computer Forensic Laboratory, National White Collar Crime Center (NW3C), and the Missouri Internet Crimes Against Children (ICAC) Task Force. I have written, executed, and assisted in over 300 search warrants on the state and federal level.
2. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. The statements in this affidavit are based on my personal observations, my training and experience, my investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited

purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252(a), and 2252A(a) are currently located at 2390 Highlandville Road, Ozark, Missouri, which is located in the Western District of Missouri.

3. I make this affidavit in support of an application for a search warrant for evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing possession, receipt, and production of child pornography. The property to be searched is described in the following paragraphs and in Attachment A. I request authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.
4. I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer in or affecting interstate commerce to receive, possess, and produce child pornography, is located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located on this property.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, relating to material involving the sexual

exploitation of minors:

- a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.
- b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.
- c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any

means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

6. The following definitions apply to this Affidavit and its Attachments:
 - a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
 - b. The term “sexually explicit conduct,” pursuant to 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
 - c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
 - d. The term “computer,” as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

- e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited

to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

i. “Domain names” are common, easy to remember names associated

with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

- j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

- 7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.
- 8. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.
- 9. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.
- 10. The computer’s ability to store images in digital form makes the computer itself an

ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet affords individuals several different venues for meeting one another, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
12. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.
13. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client

software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive

depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

BIT TORRENT PEER TO PEER (P2P) FILESHARING NETWORK

14. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets, and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users.
15. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a “torrent” file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their “infohash,” which uniquely identifies the torrent based on the file(s) associated with the torrent file.
16. To download file(s) from other users on the BitTorrent network, a user typically

obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

CELLULAR PHONES AND CHILD PORNOGRAPHY

17. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.
18. Cellular phones (“cell phones”) are exceptionally widespread. The Central Intelligence Agency estimates that in 2016 there were 416 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images and the ability to access and browse the internet.
19. In my training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and

then store the images both on the phone and on other devices – such as computers and computer storage media.

20. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

21. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:
 - a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto optics, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

- b. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
- 22. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (“CPU”). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).
- 23. Furthermore, because there is probable cause to believe that the computer, its

storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF THE INVESTIGATION

24. On December 6, 2017, Springfield Police Detective and Southwest Missouri Cyber Crime Task Force Officer (TFO) Lee Walker was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated for a device at IP address 47.213.168.188, due to its association with a torrent file known to contain at least one depiction of child pornography.
25. Using a computer running investigative BitTorrent software, a direct connection was made to the device at IP address 47.213.168.188, hereinafter referred to as the “Suspect Device.”
26. On December 6, 2017, between 1:08 a.m. and 5:21 a.m., UTC, 276 files were download from the Suspect Device. The Suspect Device was the sole candidate for each download, and as such, each file was downloaded directly from the Suspect Device.
27. I and TFO Walker reviewed the downloaded files and determined that multiple files contained depictions of children as young as five years old engaged in sexually explicit activity. Several of the files downloaded from the Suspect Device are described as follows:

- a. A file entitled “(pthc lolifuck) 10yr boy fuck 8yr sister(2)(2)(3).jpg” depicts a minor female on her hands and knees engaged in what appears to be sexual intercourse with a minor male;
- b. A file entitled “\$rkj7nil.jpg” depicts a male, approximately 13 years old, laying on a couch with a minor female, who appears to be approximately 12 years old, laying on top of him. The male’s penis is penetrating the girl’s visible vagina;
- c. A file entitled “pictures from ranchi torpedo dloaded in 2009- pedo kdv kidzilla pthc toddlers (0yo 1yo 2yo 3yo 4yo 5yo 6yo 9yo tara babyj...jpg)” depicts a female, approximately six years of age, performing oral sex upon an adult male;
- d. A file entitled “- (spda) 12 anos cojida poer el culo por su padre por webcam...avi” depicts a female, approximately 12 years old, being anally sodomized by an adult male;
- e. A file entitled “!!new (pthc) amber 7yr old bj and butplug...avi” depicts a minor female, approximately seven years old, performing oral sex on an adult male; and
- f. A file entitled “(kingpass) - marissa.avi” depicts a minor female, approximately eight years old, being orally and anally sodomized by an adult male.

28. On January 15, 2018, investigators determined that IP address 47.213.168.188 was registered to Suddenlink Communications by conducting a query of the American Registry for Internet Numbers (ARIN).

29. TFO Walker obtained and issued an investigative subpoena to Suddenlink Communications for the records on the Suspect Device for the dates and times the illicit files were made available.
30. Suddenlink Communications provided documentation establishing that the IP address was assigned to an account registered to Bob Kindrick with a service and billing address of 2390 Highlandville Road, Ozark, Christian County, Missouri, during the relevant time period. The records indicated the account was activated on November 13, 2017.
31. TFO Walker searched police records and learned that Bob Kindrick lived at the location with his son, Michael Kindrick.
32. On February 1, 2018, TFO Walker obtained Missouri Department of Revenue (DOR) and criminal history records on Michael and Bob Kindrick and fully identified them. Both subjects showed a home address of 2390 Highlandville Road, Ozark, Missouri.
33. DOR records indicated Michael Kindrick had a 2002 Chevy pickup registered in his name with Missouri license plate 5KV-315. The listed VIN showed his vehicle was possibly a Silverado 2500HD. He also had a 2007 homemade flatbed trailer registered in his name with Missouri license plate 21F-2DX.
34. Michael Kindrick's Facebook account displayed photos of a white Chevy Silverado 2500HD, with an attached black flatbed trailer loaded with a yellow, zero-turn style lawn mower.

35. On February 1, 2018, TFO Walker conducted limited surveillance of the residence. It consisted of a mobile home and a few outbuildings (car ports) positioned in the middle of a few acres of open field surrounded on all sides with trees. There was a long driveway leading from Highlandville Road to the house. A white Chevy Silverado 2500HD truck, black flatbed, and yellow zero-turn mower, were observed parked under a carport.

PROBABLE CAUSE

36. Based upon the above facts, I believe probable cause exists for the issuance of a warrant to search the premises described in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, including but not limited to the items listed in Attachment B.



Jeffrey Burnett
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn before me this 13th day of April, 2018.



David P. Rush
United States Magistrate Judge
Western District of Missouri